

Appln No. 09/690,796
Response date September 13, 2006
Reply to Office action of July 24, 2006

REMARKS/ARGUMENTS

Claims 1, 5-10, 17, 22, 42, 50-52, 55-59, 61, 92, 107, 108, 110, 113, and 114 are currently pending. No claim is amended.

Claim 56 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 1, 5-10, 16, 17, 22, 42, 50-52, 55, 57-59, 61, 92, 107, 108, 110, 113, and 114 are rejected under 35 U.S.C. 103 as being unpatentable over the following **six references**: Cordery et al. (US 6,466,921) in view of Pierce et al. (US 6,151,591) and Rosenzweig et al. (US 6,081,810) and either Gupta or Rosen and further in view of Applicant's admitted prior art (AAPA).

Applicant's attorney thanks the Examiner for the interview conducted on September 12, 2006. The claimed invention, the cited prior art, and claims 1 and 50 were discussed.

Independent claim 1 includes, among other limitations, "each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users," and "the respective cryptographic module retrieves the data record for the given user from the database." Applicant respectfully submits that none of the cited **six** references, alone or in combination teach or suggest the above limitations.

First, the limitation of "each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users," is not taught or suggested by Cordery.

Rather, each of the **Cordery's** "boxes" (40, 42, and 44 in FIG. 1) are for one of authenticating, processing value OR generating indicia data. That is, in Cordery's system, an authentication box 40 authenticates the mailer, and a different meter box 44 processes values and generates indicium data. In other words, none of Cordery's Codery's "boxes" is capable by itself of authenticating, processing value for the VBI, and generating indicia data for the plurality of users," as required by claim 1.

Appln No. 09/690,796
Response date September 13, 2006
Reply to Office action of July 24, 2006

More specifically, **Cordery's** system includes a meter box 44 that generates at least one digital token or signs the postage transaction and updates the meter record (that is, processing value) corresponding to the transaction for each postage transaction. Additionally, Cordery's system includes an authentication box 40 to authenticate a mailer; and a transaction box 42 to sign user transaction records, such as logins. (FIG. 2, and col. 7, lines 35-65, emphasis added.).

Cordery is very clear about the functions performed by each of its secure boxes located in the Data Center 30. "Function Server 34 communicates mailer records from mailer database 62 to authentication box 40, which then authenticates the mailer requesting the transaction." (Col. 8, lines 14-17, emphasis added.). "Once the mailer has been authenticated, Function Server 34 communicates the appropriate meter record 64 to meter box 44, which . . . performs accounting functions on the ascending and descending registers in meter record 64." (Col. 8, lines 17-23, emphasis added.). "Meter box 44 then generates data for an indicium, and resigns meter record 64." Col. 8, lines 24-25, emphasis added.). Accordingly, Cordery does not teach or suggest the above limitation.

Additionally, AAPA, Pierce, Rosenzweig, Gupta or Rosen alone or in combination, do not cure the above deficiencies of Cordery.

Applicant respectfully disagree with the statement in the Office action that the Background of the Invention Section (Page 2 of the Specification) suggests the above limitation. Rather, the Background of the Invention Section describe in general a software-based system and may have one or more cryptographic modules. There is nothing in that section that may teach or even suggest "each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users."

Pierce's system has "local and remote PSDs include[ing] respectively first and second unique identification, postal value storage and digital signature generator. The first client module is connected to a remote data center that includes third unique identification, third postal value storage and a third digital signature generator. The first client module selectively requests one of a first evidence of postage payment from the local PSD, a second, evidence of postage payment from the remote PSD and a third evidence of postage payment from the data center." (Abstract).

Appln No. 09/690,796
Response date September 13, 2006
Reply to Office action of July 24, 2006

However, **pierce's** system does not have a plurality of cryptographic modules in a server system. Even if the PSDs 40 may be construed as the plurality of cryptographic modules, each of those PSDs are for postage meter processing of only a portion of the users, for example, "based on matching the origin zip code of the PSD to the zip code of the return address of the mailpiece" (col. 9, lines 38-40), or based on a list of the available PSD for a particular user to select from (Col. 9, lines 2-5). Therefore, Pierce, like Cordery, does not teach or suggest "each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users," as required by claim 1.

Rosenzweig is about access control to a database and does not teach or suggest "a plurality of cryptographic modules, each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users."

Similarly, **Gupta** is directed to a method for authenticating users and does not teach or suggest "a plurality of cryptographic modules, each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users."

Likewise, **Rosen** teaches an electronic ticket presentation and transfer method in which a customer trusted agent securely communicating with a first money module, and a merchant trusted agent securely communicating with a second money module. There is no teaching or suggestion in Rosen about "a plurality of cryptographic modules, each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users."

Accordingly, Cordery, Pierce, Rosenzweig, AAPA, Gupta or Rosen, alone or in combination, do not teach or suggest the limitation of "a plurality of cryptographic modules, each of the plurality of cryptographic modules for authenticating, processing value for the VBI, and generating indicia data for the plurality of users."

Second, the limitation of wherein "**the respective cryptographic module retrieves the data record for the given user from the database**," is not taught or suggested by Cordery.

Rather, in **Cordery's** system, as clearly shown in FIG. 3 and described in the related text, **only the Function Server 34 is capable of accessing the Database Server 36**. In "step 105, Function Server 34 requests access to the mailers account information stored in Database Server 36. . . . At step 115, Function Server 34 sends the mailer information to Authentication Box 40. When the mailer is authenticated at step 120, then, at step 125, Function Server 34 sends the meter information, including the meter record to meter box 44. . . . At step 135, Function Server 34 sends the updated and signed meter record to Database Server 36 . . . " (Col. 9, lines 19-35).

Therefore, the information in the database is only accessed by the Function Server and sent to the authentication box to authenticate the mailer (step 120). The account information is then sent from the authentication box to the meter box to process value for the postage and generate indicia data for the mailer (step 130). The Function Server then stores the updated meter record back in the database.

In contrast, according to the present invention as claimed by claim 1, a "respective cryptographic module" that is, any of the cryptographic modules that is going to authenticate, process value, and generate indicia data for a given user "retrieves the data record for the given user from the database." This provides the present invention with the capability of one secure database of data records that is accessible by any of the (secure) cryptographic module (not by a less secure "Function server") for the authentication, processing value, and generating indicia data functions. Also, this requires that the claimed cryptographic modules be more complete and autonomous in their functionality and less similar to the "slave like" boxes of Cordery.

Likewise, AAPA, Pierce, Rosenzweig, Gupta or Rosen alone or in combination, do not cure the above deficiencies of Cordery.

Again, Applicant respectfully disagrees with the statement in the Office action that the Background of the Invention Section (Page 2 of the Specification) suggests the above limitation. Rather, the Background of the Invention Section describe in general a software-based system and may have one or more cryptographic modules. There is nothing in that section that may teach or even suggest "respective cryptographic module retrieves the data record for the given user from the database."

Appln No. 09/690,796
Response date September 13, 2006
Reply to Office action of July 24, 2006

Similarly, **Pierce** does not teach or suggest wherein the respective cryptographic module retrieves the data record for the given user from a secure database remote from the users including a data record for each of the users, because each PSD of Pierce has its own storage area for storing the meter information. "At step 350, the accessed PSD (local, remote or virtual) deducts the requested postal amount from a total postal value stored in the PSD and generates a signature using information supplied with the request including the addressee information. At step 355, the PSD sends transaction information including the signature to the requesting Client PC." (Col. 9, lines 26-30, emphasis added.).

Rosenzweig is about access control to a database and does not teach or suggest wherein "the respective cryptographic module retrieves the data record for the given user from the database."

Again, **Gupta** is directed to a method for authenticating users and does not teach or suggest wherein "the respective cryptographic module retrieves the data record for the given user from the database."

Rosen teaches an electronic ticket presentation and transfer method in which a customer trusted agent securely communicating with a first money module, and a merchant trusted agent securely communicating with a second money module. There is no teaching or suggestion in Rosen about wherein "the respective cryptographic module retrieves the data record for the given user from [a] database" that is "remote from the users including a data record for each of the users."

Consequently, Cordery, AAPA, Pierce, Rosenzweig, Gupta or Rosen, alone or in combination, do not teach or suggest the limitation of wherein "the respective cryptographic module retrieves the data record for the given user from the database," as required by claim 1.

At least, for each of the above two reasons, claim 1 is patentable over combination of Cordery, Pierce, Rosenzweig, Gupta or Rosen.

Amended independent **claim 50** includes, among other limitations, "retrieving the data record for a given user from the database for authenticating the given user; retrieving for a second time the data record for the given user from the database for processing value for the VBI

Appln No. 09/690,796
Response date September 13, 2006
Reply to Office action of July 24, 2006

for the given user; updating, and storing back in the database ,the data record for the given user after processing value for the given user; retrieving for a third time the updated data record for the given user from the database for generating indicia data for the given user; and updating, and storing back in the database, the updated data record for the given user after generating indicia data for the given user."

As discussed above, Cordery's Function Server 34 accesses the database only once for each transaction (See, for example, FIG. 3, step 110). This information is then sent to the authentication box to authenticate the mailer (step 120) and to meter box to authenticate meter record (step 130).

Therefore, Cordery does not teach or suggest "retrieving for a second time the data record for the given user from the database for processing value for the VBI for the given user" or "retrieving for a third time the data record for the given user from the database for generating indicia data for the given user."

Additionally, Cordery does not teach or suggest "updating and storing back in the database the data record for the given user after processing value for the given user," or "updating and storing back in the database the updated data record for the given user after generating indicia data for the given user," because Cordery's system does the updating and storing back only once after all of the needed processes are completed. (See, for example, FIG. 3, step 140 and col. 9, lines 23-39).

In contrast, the present invention as claimed by claim 50, updates and stored back the user record after it processes value and again updates and stored back the user record after the indicia data is generated. That is, after each of the value processing and indicia data generation processes, is completed, the data is updated and stored back in the database. This adds more data security to the system.

Similarly, Pierce, AAPA, Rosenzweig, Gupta, or Rosen, alone or in combination with Cordery, do not teach or suggest the above limitations. Consequently, independent claim 50 is also patentable over cited references.


Appln No. 09/690,796
Response date September 13, 2006
Reply to Office action of July 24, 2006

Independent **claims 92 and 107** include similar patentable limitations and therefore, they are also patentable over cited references.

Dependant claims 5-10, 17, 22, 42, 51-52, 55-59, 61, 108, 110, and 113-114 depend directly or indirectly from respective allowable claims 1, 50 and 107, and thus are allowable as are claims 1, 50 and 107, and for additional limitations recited therein.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By 
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS700364.1-*-09/13/06 9:09 AM